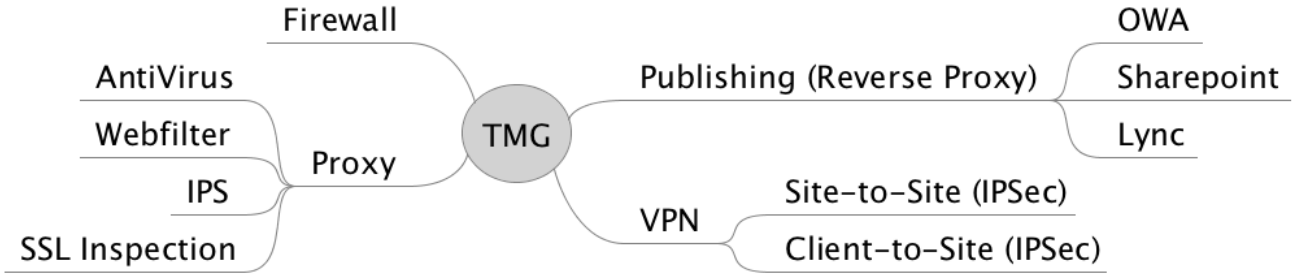
# Microsoft TMG Replacement

## How FORTINET integrated secuity platforms Help Protect the Perimeter in a Microsoft Infrastructure Environment

## 1. Introduction

This document gives an overview of FortiGate features and models which are relevant when it comes to choosing a successor for Microsoft's TMG.

The main focus is placed on the following TMG functions:




Besides FortiGate as an Integrated Security System/Next Generation FW, alternate products from Fortinet's portfolio may be used in certain cases:

- Web Application Firewall (FortiWeb)
- Mail Security (FortiMail),
- Loadbalancer (FortiBalancer)

This document focuses on replacing the most common TMG functions with FortiGate platforms, and achieving an easy to administer and cost effective solution for the SME market.

Fortinet appliances´ simple license model is of particular interest. Specifically, FortiGate is not licensed on features or on functions. All features[1] are available without additional costs. Therefore the selection of the right model is mainly based on throughput. Additional services such as hardware and software support, as well as definition updates for AntiVirus, IPS, Application Control, URL filtering, etc. can be added when required.

A list of authorized EMEA Fortinet Distributors is available here:
http://www.fortinet.com/partners/emeapartners.html

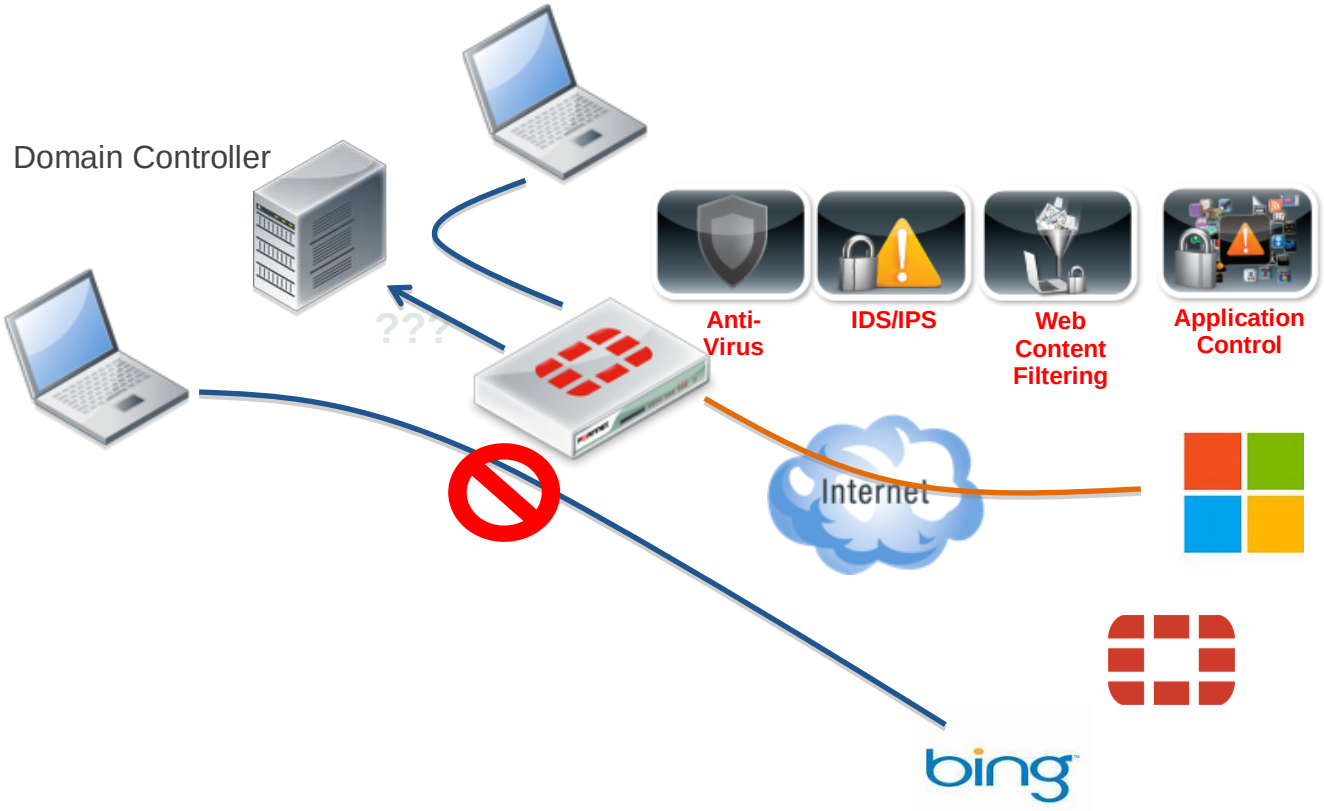
Further information can be found on the following Fortinet websites:
http://www.fortinet.com
http://docs.fortinet.com
http://kb.fortinet.com
http://www.fortinet.com/partners/partner_program/fppemea.html

[1] Due to technical capabilities, the FortiGate-60C/D and models below offer a limited feature set. Details are pointed out in Chapter 3.

## 2. TMG features

### a. Proxy

One of the oldest and most-used functions of TMG was the role as a proxy server to enable Internet access for clients. In this context a key aspect was that users did not have to sign-in a second time.
This Single-Sign-On (SSO) feature is part of the FortiGate feature set and is fully integrated. Thereby the FortiGate communicates with the Active Directory domain controllers and is able to read and evaluate the rights and permissions of users signed-in. Additionally comprehensive security functions including AntiVirus, Intrusion Prevention, Web Filter and Application Control can be used.



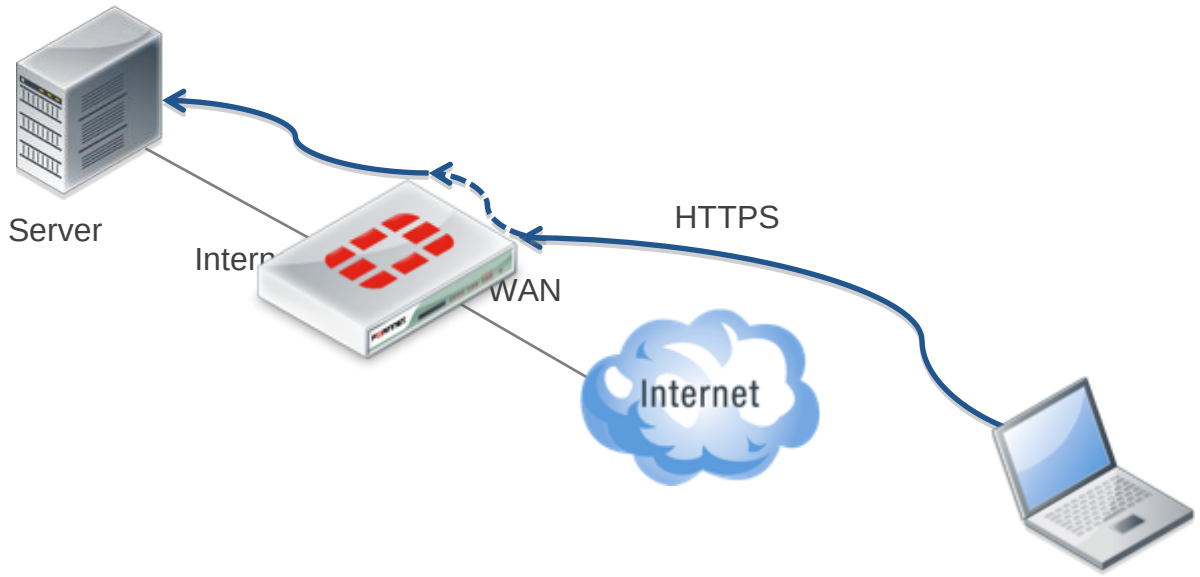

Today almost every application tries to communicate via HTTP or HTTPS with various servers on the Internet. With application control enabled, the IP traffic and packets are inspected in detail. Thus FortiGate allows for detecting and differentiating between various applications, for example Skype, Skydrive, WindowsUpdate, NetMeeting, and many more. Detection is of course not limited to a particular vendor. Numerous applications are recognised as either dangerous or potentially harmful programs, such as botnet activity, remote access or file sharing applications.

The latest list of applications is available at http://www.fortiguard.com

### b. OWA/SharePoint Publishing

From a functional perspective, two things are important when it comes to publishing Outlook Web Access or SharePoint services:

- Translation of the public IP address
- Exchanging the certificate, that external clients receive a valid, trusted and signed certificate.
- Exchanging the certificate: ensuring that external clients receive a valid, trusted and signed certificate

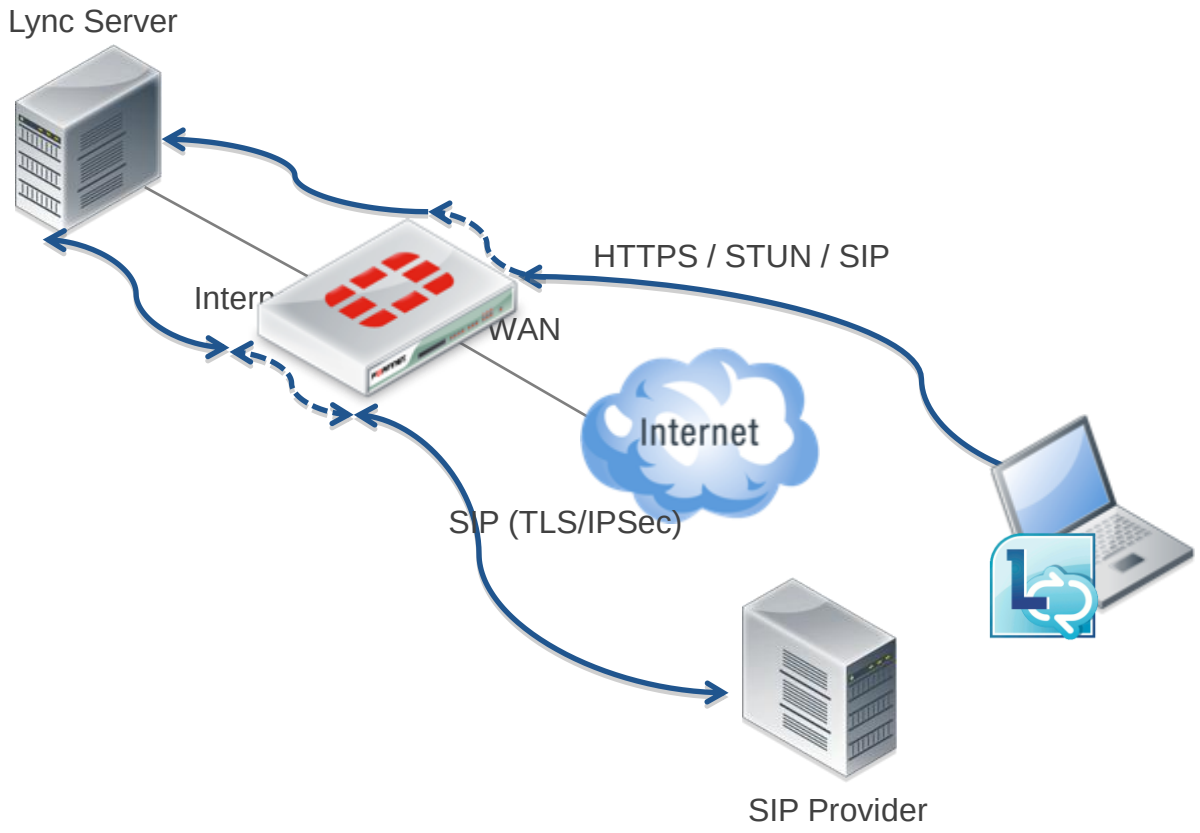



When it comes to securing the application, the following security features are a good extension:

- Scanning for attacks (Intrusion Prevention System)
- Scanning for viruses
- Checking of used paths for HTTP applications
- Verifying communication protocol in use (is it HTTP(S) or Activesync traffic/packets?)
- Blocking IP address and/or alarm administrators upon failed login attempts
- Load sharing when using multiple application servers

### c. Lync Publishing

When publishing Lync services, there are more communication protocols in use compared to OWA/SharePoint. However infrastructure service requirements remain the same. Once again we see that public IP addresses need to be translated and SSL certificates changed accordingly on the perimeter side.




From a security standpoint, requirements increase due to the additional communication protocols involved. The perimeter firewall needs to be able to verify all of these protocols.

This results in the following features list:

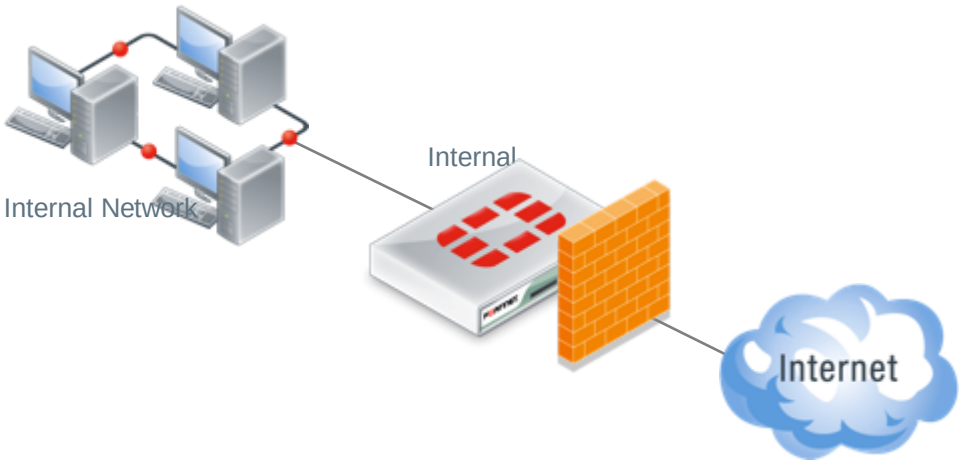
- Scanning for attacks (Intrusion Prevention System)
- Scanning for viruses
- Checking of used paths for HTTP applications
- Verifying communication protocol in use (is it HTTP(S) or Activesync traffic/packets?)
- Layer 7 analysis of VoIP data
- Blocking of IP address and/or alarm administrators upon failed login attempts
- Load sharing when using multiple application servers

Within the FortiGate feature set, a SIP (TLS) application level gateway (ALG) has been implemented, which enables detailed inspection and filtering of SIP traffic.

### d. Firewalling with Fortinet FortiGate

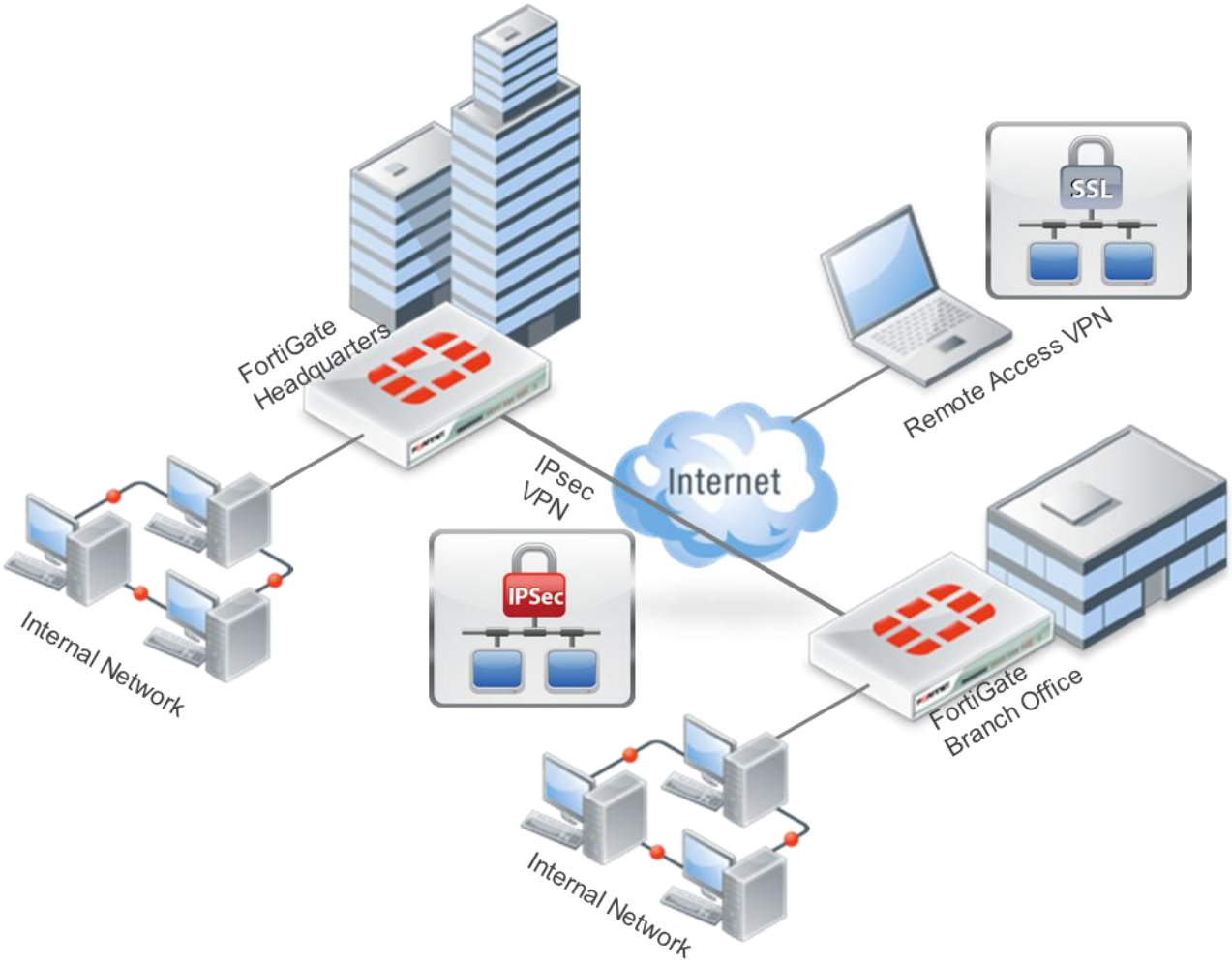
An Integrated Security System/Next Generation Firewall is the first line of defence against Internet attacks, providing protection for internal resources. At the same time, unwanted communications sent externally must be prevented.

The core of all FortiGate models is the FortiOS operating system which serves as a platform for numerous fully-integrated security functions. These systems defend against advanced attacks and the latest threats. Established policies control all data flow that encounters a FortiGate appliance. Stateful-Inspection firewall supplemented by security components such as AntiVirus, IPS, Application Control, Webfilter, etc. ensures secure communication. Numerous industry certifications and recognitions prove the superiority of FortiGate appliances. The FortiGate's ability to build identity-based firewall policies (based on user or group information) is homogenous with Microsoft infrastructure environments using central user authentication and Single-Sign-On.



### e. Virtual Private Networks with Fortinet's FortiGate

Virtual Private Networks (VPN) allow secure, encrypted communication with company networks and resources. This means users can connect from outside the office and establish a secure connection from their smartphone or notebook using SSL VPN. The connection of various office locations can be achieved using persistent IPSec VPN tunnels.




Fortinet's FortiGate offers remote access for mobile workers using SSL-VPN or L2TP/IPSec, and IPsec VPN for typical site-to-site communications between multiple locations. Pre-shared keys certificates are supported for authenticating devices and users. FortiToken is a one-time password solution directly built into the FortiGate operating system. It allows two factor authentication to securely authenticate mobile users.

## 3. Fortinet Products/Feature Matrix

Fortinet's broad range of FortiGate models offers a flexible and effective choice of products to protect company networks. Due to the diversity of the different models, solutions are available for the smallest offices (1-5 users) to enterprise environments (10,000 users and more).

An overview of all current FortiGate models can be found on the Fortinet Homepage at
http://www.fortinet.com/products/fortigate/

Depending on the TMG features and throughput required, as an example for small networks, the following FortiGate models should be considered when replacing TMG:

| Model | Firewall | VPN | Client-Proxy | OWA/SPS Publishing | Lync Publishing |
|---|---|---|---|---|---|
| **FortiGate-60C/D** | Yes | Yes | Yes | No | No |
| **FortiGate-100D** | Yes | Yes | Yes | Yes | Yes |

| | Firewall (1518/512/64 byte) | Concurrent Sessions | New Sessions/Sec | IPSec VPN | IPS (HTTP) | Antivirus (Proxy/Flow) |
|---|---|---|---|---|---|---|
| **FortiGate -60D** | 1.5 /1.5 /1.5 Gbps | 500K | 3.200 | 1 Gbps | 200 Mbps | 35 /50 Mbps |
| **FortiGate -100D** | 2500 / 1000 / 200 Mbps | 2.5 Mil | 22.000 | 450 Mbps | 950 Mbps | 300/700 Mbps |